REMARKS

After the foregoing Amendment, Claims 1-8, 10-12, 14-27, and 32-33 are currently pending in this application. Claims 1, 4, 10-12, and 15-27 have been amended to more distinctly claim subject matter which the Applicant regards as the invention. Claims 28-31 have been canceled. Clams 32-33 have been added. No new matter has been introduced into the application by these amendments.

In particular, claims 1 and 10 have been amended to recite automatically generating by the first secure module a root or super-root key request in dependence on a root or super-root key status, respectively, and transmitting the request; and transferring the requested keys responsive to the request. Claims 15 and 21 have been amended to recited a secure module comprising a root key or super-root key generator, respectively, for generating a root or super-root key request in dependence on a root or super-root key status. Support is found in paragraphs **[035]**, "Module **10** receives a signal to generate a root key request at step **100** in dependence upon a current root key status. For example, the signal is sent to module **10** when the root key is compromised or after a predetermined root key usage limit is achieved. The module **10** generates a root key request ..."; and **[038]**, " ... key replacement after key compromise is implemented automatically by code internal to a secure cryptographic module..."; and **[039]**, "... two super root keys are provided within each module wherein one of the super-root keys is for replacing the other super-root key thereby providing a system to allow replacement of all symmetric super-root keys in all modules upon any indication of key compromise or at intervals when desired."

Claim Rejections - 35 U.S.C. § 103

Claims 1-8, and 15-18, stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Davies et al. (Security for Computer Networks, hereinafter "*Davies*") in view of Arnold (US Patent No. 6,148,400, hereinafter "*Arnold*"). This rejection is respectfully traversed.

To establish a *prima facie* case for obviousness under 35 USC § 103(a), it must at least be shown that the asserted references, when read alone or in combination, teach all of the elements of the examined claims.

The current application is directed to methods and apparatus for providing for secure transfer of private root keys and private super-root keys between a key provider system and a second other system over a network that is other than secure (such as the Internet). The second other system is provided with or is in communication with a secure module that comprises a processor, input, memory circuit and storage, and a root key or super-root key request generating module. The transfer of root keys and super-root keys is in response to requests generated automatically by the secure module in dependence on a root key or super-root key status, respectively. None of the cited references suggests such a secure module that automatically requests replacement root keys and super-root keys in dependence on a root key or super-root key status. Therefore, the 35 USC § 103(a) rejection is not supported.

In particular, as is appreciated by one of skill in the art, the second other system communicates securely with client stations by the use of private/public encryption key pairs which are used to encrypt/decrypt confidential data that is passed between the second other system and the client stations. In addition, the second other system communicates securely with the key provider by the use of root key pairs and super-root key pairs. The root keys are used for replacing encryption keys, which are provided by the key provider for use by the second other system. The super-root keys are used for replacing root keys or other super-root keys, all of which are provided by the key provider for use by the secure module. The root keys and super-root keys stored in the secure module are always private keys.

Replacement encryption keys, root keys, and/or super-root keys might be provided, for example, if the keys in use become compromised, or in accordance with procedures such as replacement of the keys at desired intervals to reduce the likelihood that they will become compromised.

Advantageously, the security of the root keys and super-root keys is maintained by the key provider. "The module is accessible only by the provider and as such is completely secure against unauthorized entry," (see, e.g., lines 3-6 of paragraph **[015]**). In particular, "any external attempts to probe the electronic contents of the module **10**, by electronic or mechanical methods, deactivates the module and erases the secure data stored therein, including the private super root key. Accordingly, external access to the private super-root key is avoided at all times," (paragraph **[030]**, lines 12-16). Thus, there should be no way that the super-root key can be compromised by the second other system. In this manner, the security of the root keys and super-root keys is maintained by the key provider, and not by the second other system.

Nevertheless, in another embodiment, an additional private super-root key is provided in the secure module for use, e.g., in the extremely unlikely event the original super-root key does indeed become compromised, or is to be replaced for any reason, such as at desired intervals.

The Examiner cites *Davies* for various features of the claimed invention which Applicant is unable to find at the cited locations. In a first portion of *Davies* is disclosed a scheme for computer network security in which a "host is responsible for a group of terminals. The host acts as a key distribution centre for its own group of terminals and encipherment is used for messages passing between the terminal and the host... Each terminal contains a terminal key *kt* and at the start of a communication session a session key *ks* is delivered to it, enciphered under the terminal key." (page 144 lines 14-16, 26-28.) In contrast in the current application, there are no separate session and terminal keys for use by terminals. In *Davies*, "the host computer is provided with a special, physically secure module [called] a 'Tamper Resistant Module' (TRM)... At the host all encipherment operations occur <u>inside</u> the TRM" (page 144 lines 36-39). In contrast in the present application, encryption keys can be provided by the encryption unit **3** to the network server **2** for use <u>outside</u> of the encryption unit for secure communications with client stations **4**.

In this portion of *Davies*, "there is a three-level key hierarchy... At the top level are two master keys, *km*0 and *km*1. In the middle level are the terminal keys, denoted *kt*, one for each terminal belonging to the host. The lowest level keys are the session keys, *ks*, which are associated with terminals on a more temporary basis. Only the session keys encipher data. The terminal keys [] are used to encipher session keys for transmission to the terminals." (page 145 lines 38-46.) Thus, two levels of the key hierarchy (session keys and terminal keys) are used to establish secure communications between the host and the terminals. In addition, there are two "master" keys. The use of the two master keys is not apparent from this portion of *Davies*. Nevertheless, this key hierarchy is clearly different from the key hierarchy of the present application, wherein only one level of the hierarchy (the encryption keys) is used to establish secure communications between the computer system **1** and the client stations **4**. In addition in the present application, two levels of the hierarchy (both the super-root keys and the root keys) are used to provide secure communications between the computer system **1** and the key provider, which doesn't even exist in this portion of *Davies*.

In a subsequent portion of *Davies*, "each participating [] organization is expected to have a *key management facility* which includes the cryptographic equipment and provides a secure environment in which the cryptographic functions can be performed and the keys held." (page 158 lines 35-38.) As described above, *Davies* discloses a "host" which provides such a secure environment, which host acts as a key distribution centre for its own group of terminals, and which is provided with a TRM in which all encipherment operations occur, and the host appears to be analogous to the network server **2** of the present application. There does not appear to be anything in this portion of *Davies* analogous to the "key provider system" of the present application, which is present in all claims. This is not surprising, since *Davies* explains a standard which "does not describe how secure arrangements can be made for the storage of the keys, though their encipherment under some unspecified master key is implied. These [] details [] are not specified because they do not affect the exchange of messages between the participants." (page 158 lines 38-42.) In contrast, such details are indeed recited in the claims.

Furthermore, in *Davies*, apparently the only method of distributing keys actually referred to with particularity is in "a short section of the standard, little more than one page together with an example in an annex, [which] deals with the manual distribution of keying material which sets up the basic keys on which the key hierarchy depends." (page 158 lines 43-45.) Thus, *Davies* appears to suggest that the security keys be typed into the system manually before they are distributed by the host and/or used for secure communications. In contrast in the present application, keys are automatically generated.

Davies then goes on to describe a two or three layered hierarchy of keys (pages 159-160), which are distributed in one of three key distribution environments (pages 161-165). "A key used for enciphering [] data is known as a *data* key (DK) … For the distribution of data keys, a *key encrypting key* (KK or KKM) is used… In the three-layer hierarchy any KK which is used to encipher a data key for transmission can itself be distributed using a master key encrypting key (KKM)." (page 159 line 36 - page 160 line 4.) In this portion of *Davies*, "it is possible to use a key management centre which has an established cryptographic relationship with both parties to the communication. Then, using the key already established they can obtain the necessary material from the key management centre to establish contact. There are two kinds of key management centre, one of which generates keys, called a *key distribution centre* and the other which accepts a key from one party, re-encyphers it and returns it [], called a *key translation centre*. Thus there are three environments in the standard, [one of which is known as a] *key distribution centre…*" (page 161 lines 18-26.) The procedures for carrying out key distribution using the key distribution center model are disclosed on pages 163-164. The key distribution center appears to be somewhat analogous to the key provider of the current application. However, the disclosed procedures are easily distinguished from the procedures in the current application.

In particular, in *Davies*, in an example in which two banks want to communicate securely, "if bank A does not have a data key in common with bank B it may be able to establish such a key through the agency of a key distribution centre (CKD). For this purpose, bank A first communicates with the distribution center and obtains from it a new data key in two forms. One of these it can interpret using a KK which it holds in common with the distribution centre. The other it passes on to the bank B which itself can interpret this using another KK which it has in common with the same distribution centre." (page 163 lines 37-43.) Thus, both parties A and B are in direct communication with the distribution centre. This configuration is clearly different from the present application, wherein the key provider provides encryption keys to the computer system **1** (using root keys), the computer system **1** provides them to the client station **4**, and the client station does NOT communicate directly with the key provider. In addition *Davies* states, "note that a key distribution centre does not supply key encryption keys." (page 164 lines 8-9.) This again is easily distinguished from the present application, wherein the key provider does indeed supply root keys.

In an alternate configuration called a key translation centre, (*Davies* bottom of page 164 to page 165), "bank A generates the keys it needs and passes them to the translation centre for conversion to encipherment under the keys held in common between that centre and bank B." Thus in this configuration, in contrast to the claims, not only is bank B in direct communication with the key translation centre, but the keys are not even generated by the key translation centre. Instead, the keys are generated by bank A. Clearly, this is different from the present application, wherein the keys are indeed generated by the key provider, provided to the network server, and used for secure communication between the network server and client stations, and there is no direct communication between the client stations and the key provider.

Thus it can be seen that there is no direct analogy between the elements of the present application and allegedly similar elements the Examiner contends can be found in *Davies*. In particular, with regard to claim 1, the Examiner contends that *Davies* discloses "a) encrypting the first root key using a first super-root key of the key provider system" and "c) transferring the encrypted first root key from the key provider system to the second other system via the information network." This is incorrect. Instead, as discussed above, in one portion *Davies* discloses a system that does not even have a key provider system as that term is used in the present application. In another portion *Davies* discloses configurations having either a key translation center or a key distribution center, neither one of which provides a "root key encrypted using a super-root key of the key provider system." In the configuration in *Davies* having a key distribution center, for example, in which the key distribution center appears to be analogous to the key provider system of claim 1, steps a) and c) require that the key distribution center must provide the first root key, encrypt it, and send it to the host. Instead, as described above, in this configuration "a key distribution centre does not supply key encryption keys" (page 164 lines 8-9). And, in the configuration having a key translation center, in which the key translation center appears to be analogous to the key provider system of claim 1, "bank A generates the keys it needs and passes them to the translation centre…" (page 164 lines 34-35). This is essentially the opposite of what is recited in claim 1, wherein the keys are encrypted by the key provider system and transferred to the second other system.

The Examiner contends steps a) and c) are found on "pages 162 and 163," but Applicant is unable to find them there or elsewhere in *Davies*. Applicant respectfully requests the Examiner specify with particularity where these features are found in *Davies*. Similarly, the Examiner contends step d) is found in *Davies* on "pages 162 and 163", and step e) is found in *Davies* on "pages 160-163," but Applicant is also unable to find those steps at the referenced locations or elsewhere in *Davies*. Applicant respectfully requests the Examiner specify with particularity where those steps are found in *Davies*.

In addition, *Davies* discloses "data keys are always single length keys" (page 159 lines 43-44), and "the use of double-length keys is mandatory only for master keys which are used for key management between a participant and one of the two kinds of key management centre," whereas "key encrypting keys (KK or KKM) can be either single or double length but a single length key must not be used to encipher a double length key" (page 160 lines 12-17). The Examiner contends that "*Davies* teaches the idea that a key encrypting key should be twice as long as the key it is encrypting" (page 12 of the Action), from which the Examiner deduces that *Davies* teaches the length L of the KK is twice as long as the key it encrypts, and the KKM is twice as long as the KK. This is incorrect. Instead, as indicated above, *Davies* teaches that data keys (i.e., encryption keys) are always single length keys, a KKM used in any configuration analogous to the claims (i.e., super-root keys) must be double-length, and the KK can be either single or double length. *Davies* clearly does not anticipate under any circumstances a KKM that is four times as long as a data key, and Applicant respectfully submits it is only with impermissible hindsight that the Examiner suggests *Davies* discloses that it does. See MPEP 2143.01.

The Examiner admits that *Davies* fails to disclose the use of a secure module in the second other system having a second super-root key within a read-only memory circuit thereof. The Examiner relies on *Arnold* for this feature. However, *Arnold* discloses only that "the public key of the MKS [master key station, apparently analogous to the computer system **1** of the current application] **100** will be programmed into read-only memory (ROM) on the secure chip **140** to provide permanent storage of this key" (column 8 lines 63-65). *Arnold* uses a <u>public</u> key because the key is used for verification, as noted, e.g., in column 4 lines 2-10, and a public key is used to verify the authenticity of a message generated with an associated private key, as would be appreciated by one of skill in the art.

In contrast, in claim 1 the ROM of the secure module stores a super-root key that is a <u>private</u> key. As recited in claims 5 and 6 respectively, the private key may be a private key of a private/public key pair, or a private key for use with a symmetric key-based encryption algorithm. The Examiner contends that attempting to combine *Davies* with *Arnold* to form claims 1, 5 and 6, would have been obvious to one of skill in the art. Applicant respectfully disagrees. *Arnold* stores a public key in its secure chip because *Arnold* is directed to using the stored key for verification purposes. In contrast, the key stored in the secure module of the claimed invention is always a private key, because it is used for secure decryption purposes and not for verification purposes. If the public key of *Arnold* were replaced with a private key, then *Arnold* would be rendered useless for its intended purpose, because a private key cannot be used for verification of authenticity by a message recipient, as is appreciated by one of skill in the art. It is therefore impermissible for the Examiner to suggest such a combination. See MPEP 2143.01(V), "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification."

For at least the reasons presented above, independent claims 1 and 15 are deemed allowable over the cited prior art. Claims 2-8 and 16-18 depend from claims 1 and 15, respectively. Therefore, without prejudice to their individual merits, those claims are also allowable for the same reasons. In addition, independent claims 10 and 21 are similar to claims 1 and 15 with regard to the remarks presented above, and the additional prior art cited pertaining to claims 10 and 21 do not supplement the cited prior art with regard to the remarks presented above. Therefore, for at least the same reasons, those claims and their dependents are also allowable over the cited prior art.

In addition with regard to claim 5, the Examiner contends it would have been obvious to combine *Davies* and *Arnold* because the use of a public key gives the advantage of only having to keep one key private. That may or may not be true, but it has nothing to do with the reason *Arnold* discloses using a public key in a secure module, nor with the reason the claimed invention uses a private key in a secure module. As noted above, *Arnold* uses a public key in its secure chip **140** for verification purposes. In contrast, the claimed invention uses a private key in its cryptographic module **10** for decryption purposes. As would be appreciated by one of skill in the art, these are disparate and non-interchangeable uses of public and private keys.

In addition, with regard to claims 4 and 16-18, the Examiner contends that the modified *Davies* and *Arnold* system implies that since the key is only used to encrypt other keys it wouldn't be used unless it is requested. Applicant respectfully disagrees. As shown above, it is not obvious to combine *Davies* and *Arnold*, therefore no such combined system would exist to imply anything. In addition, even if it did, just because a system can be used to encrypt other keys when requested, does not imply that it would only encrypt other keys when requested, as recited in claim 4. Furthermore, claim 4 recites the processor internal to the module access the second encryption key only in response to a request from a corresponding secure module. Neither *Davies* nor *Arnold*, either alone or in any possible combination, discloses or suggests such a corresponding secure module.

For these reasons also, claims 4, 5, and 16-18 are deemed allowable over the cited prior art.

Claims 10-12 and 14 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified *Davies* (same as above) and *Arnold* (same as above) as applied to claims 1, 6, and 15, and further in view of Spelman *et al.* (U.S. Patent No. 5,680,458, hereinafter "*Spelman*").

Regarding independent claim 10, it is noted that the Examiner appears to reject claim 10 based on the rejection of claim 1, and to rely on *Spelman* only for the additional features of claim

10. In particular, the Examiner admits that the modified *Davies* and *Arnold* system fails to disclose second and third encryption keys being stored, and relies on *Spelman* for this feature. However, as described above, the modified *Davies* and *Arnold* system does not include all of the features of claim 1. Furthermore, *Spelman* does not supplement *Davies* and *Arnold* to provide all of the features of claim 1. Therefore, claim 10 is deemed allowable over the combination of *Davies, Arnold* and *Spelman* for at least the same reasons claim 1 is allowable over *Davies* and *Arnold* alone.

In addition, the examiner contends *Spelman* teaches "second and third encryption keys" being stored, citing column 2 lines 4-17. However, that is not what is recited in claim 10, nor is it what is disclosed at the cited location in *Spelman.* Claim 10 recites "a first secure module having second and third super-root keys [not encryption keys as contended by the Examiner] within a memory circuit thereof." In contrast, *Spelman* discloses replacing one of "a plurality of root keys," but has nothing to say about providing more than one super-root key (which are used to provide replacement root keys) as recited in claim 10, or about replacing a super-root key as recited in claim 11.

Spelman is directed to the problem of replacing a compromised root key of a central authority in a secure system. In *Spelman*, the parties to secure communications include the public (apparently analogous to the client stations of the present application), a certifying authority (apparently analogous to the computer system having a network server of the present application), and a central authority (apparently NOT analogous to the key provider of the present application, but instead an authority that certifies to the public the genuineness of a replacement root key provided by the certifying authority, i.e., somewhat similar to the key distribution center configuration of *Davies*, described above). *Spelman* is concerned with recovering from a compromise of root keys of the central authority, which are not super-root keys as that term is used in the present application. *Spelman* discloses generating by the central authority a message indicating a root key has been compromised and also containing a replacement root key, generating a digital signature using the compromised root key, and publishing in an out-of-band channel a value V derived from the message. In contrast, the present application is not concerned with a compromise of the security of the key provider. Furthermore, the present application solves the distinct problem of replacing a compromised root key of a network server computer system (not the key provider) simply by sending a new root key from the key provider to the network server computer system, using a previously distributed and secured super-root key. *Spelman* does not disclose or suggest the use of such a super-root key. Therefore, of course, *Spelman* does not disclose the use of a plurality of super-root keys, as contended by the Examiner.

For these reasons also, claims 10-12 and 14 are deemed allowable over the cited prior art.

Regarding independent claim 21, it is noted that the Examiner appears to reject claim 21 based on the rejection of claim 10, and to rely on Mason *et al.* (US 6,331,784, hereinafter "*Mason*") for the additional features of claim 21. In particular, the Examiner admits that the modified *Davies*, *Arnold*, and *Spelman* system fails to disclose the keys only being erasable by the program code, and relies on *Mason* for this feature. However, as described above, the modified *Davies*, *Arnold*, and *Spelman* system does not include all of the features of claim 10. Furthermore, *Mason* does not supplement *Davies*, *Arnold*, and *Spelman* to provide all of the features of claim 10. Therefore, claim 21 is deemed allowable over the combination of *Davies, Arnold, Spelman* and *Mason* for at least the same reasons claim 10 is allowable over *Davies, Arnold* and *Spelman* alone.

Claims 19-20 and 22-31 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over one or more of the references cited above, in view of one or more of Easter *et al.* (US 5,559,889), Bergum *et al.* (US 5,249,227), Ehrsam *et al.* (US 4,386,234) and Ober *et al.* (US 6,307,936). These rejections are respectfully traversed. Claims 28-31 have been canceled, mooting the rejection as to those claims.

For at least the reasons presented above, independent claims 1, 10, 15, and 21 are deemed allowable over the cited prior art. Dependent claims 19-20 and 22-27 each depend from one of those independent claims. In addition, the additional prior art cited with regard to claims 19-20 and 22-27 does not supplement the prior art cited with regard to the remarks presented above. Therefore, for at least the same reasons presented above, 19-20 and 22-27 are also deemed allowable over the cited prior art.

In addition to the remarks above, Applicant respectfully submits there is no teaching or suggestion in any of the cited references to combine their features in the manner suggested by the examiner, nor is there any standard practice in the art that would lead one of ordinary skill to combine their features. Therefore, it is respectfully submitted that it is only with impermissible hindsight that the examiner has combined the cited references. See MPEP § 2143.01.

Based on the arguments presented above, reconsideration and withdrawal of the 35 U.S.C. § 103(a) rejection of claims 1-8, 10-12, and 14-27 are respectfully requested.

Conclusion

In view of the foregoing amendment and remarks, Applicant respectfully submits that the present application, including claims 1-8, 10-12, 14-27, and 32-33, is in condition for allowance and an early notice of allowance is respectfully requested.

If the Examiner believes that any additional minor formal matters need to be addressed in order to place this application in condition for allowance, or that a telephone interview will help to materially advance the prosecution of this application, the Examiner is invited to contact the undersigned by telephone at the Examiner's convenience.

Respectfully submitted,

BRUNO COUILLARD

BY: ______________________
GREGORY J. LAVORGNA
Registration No. 30,469
DRINKER BIDDLE & REATH LLP
One Logan Square
18th and Cherry Streets
Philadelphia, PA 19103-6996
Tel: (215) 988-3309
Fax: (215) 988-2757
Attorney for Applicant